الاختراق

تعريفه و دوافعه و أنواعه و آثاره

المقدمة:

الاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف وبطبيعة الحال هي سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الأخرين عنوه ودون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية أو بنفسياتهم عند سحب ملفات وصور تخصهم وحدهم.

دوافع الاختراق :

لم تنتشر هذه الظاهرة لمجرد العبث وإن كان العبث وقضاء وقت الفراغ من أبرز العوامل التي ساهمت في تطورها وبروزها الي عالم الوجود . وقد أجمل من المؤلفين المتخصصين في هذا المجال

الدوافع الرئيسية هي:

للاختراق في ثلاث نقاط أوجزها هنا على النحو التالي :

1-الدافع السياسي والعسكري : مما لاشك فيه أن التطور العلمي والتقني أديا إلي الاعتماد بشكل شبة كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية. فمنذ الحرب الباردة والصراع المعلوماتي و التجسسي بين الدولتين العظميين آنذاك على أشده. ومع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية للأنظمة والدول ، أصبح الاعتماد كليا على الحاسوب الآلي.

وعن طريقه اصبح الاختراق من اجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية .

2-الدافع التجاري :من المعروف أن الشركات التجارية الكبرى تعيش هي ايضاً فيما بينها حربا مشتعلة (الكوكا كولا والبيبسي كولا على سبيل المثال) وقد بينت الدراسات الحديثة أن عددا من

كبريات الشركات التجارية يجرى عليها أكثر من خمسين محاولة اختراق لشبكاتها كل يوم .

3-الدافع الفردي :بدأت أولى محاولات الاختراق الفردية بين طلاب الجامعات بالولايات المتحدة كنوع من التباهي بالنجاح في اختراق أجهزة شخصية لأصدقائهم ومعارفهم و ما لبثت أن تحولت تلك الظاهرة إلي تحدي فيما بينهم في اختراق الأنظمة بالشركات ثم بمواقع الانترنت. ولا يقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية .

بعض الأفراد بشركات كبرى بالولايات المتحدة ممن كانوا يعملون مبرمجين ومحللي نظم تم تسريحهم من أعمالهم للفائض الزائد بالعمالة فصبوا جم غضبهم على أنظمة شركاتهم السابقة مقتحميها ومخربين لكل ما تقع أيديهم علية من معلومات حساسة بقصد الانتقام . وفي المقابل هناك هاكرز محترفين تم القبض عليهم بالولايات المتحدة وبعد التفاوض معهم تم تعيينهم بوكالة المخابرات الأمريكية (CIA) وبمكتب التحقيقات الفيدرالي (FBI)وتركزت معظم مهماتهم في مطاردة الهاكرز وتحديد مواقعهم لإرشاد الشرطة إليهم .

أنواع الاختراق :

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة إلي ثلاثة أقسام :

1-اختراق المزودات أو الأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية وذلك باختراق الجدران النارية التي عادة توضع لحمايتها وغالبا ما يتم ذلك باستخدام المحاكاة Spoofing وهو مصطلح يطلق على عملية انتحال شخصية للدخول إلي النظام حيث أن حزم الـــ IP تحتوي على عناوين للمرسل والمرسل إليه وهذه العناوين ي هي ذاتها التي نجع بها مخترقي الهوتميل في الولوج الي معلومات النظام قبل فترة قريبة من الزمان .

2-اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات وهي طريقة للأسف شائعة لسذاجة اصحاب الأجهزة الشخصية من جانب ولسهولة تعلم برامج الاختراقات وتعددها من جانب اخر .

3-التعرض للبيانات اثناء انتقالها والتعرف على شيفرتها إن كانت مشفرة وهذه الطريقة تستخدم في كشف ارقام بطاقات الأئتمان وكشف الأرقام السرية للبطاقات البنكيه ATM وفي هذا السياق نحذر هنا من امرين لايتم الأهتمام بهما بشكل جدي وهما

عدم كشف ارقام بطاقات الأئتمان لمواقع التجارة الألكترونية إلا بعد التأكد بألتزام تلك المواقع بمبدأ الأمان .

أما الأمر الثاني فبقدر ماهو ذو أهمية أمنية عالية إلا أنه لايؤخذ مأخذ الجديه . فالبعض عندما يستخدم بطاقة السحب الألي من آلات البنوك النقدية ATM لا ينتظر خروج السند الصغير المرفق بعملية السحب أو انه يلقي به في اقرب سلة للمهملات دون ان يكلف نفسه عناء تمزيقه جيدا . ولو نظرنا إلي ذلك المستند

سنجد ارقاما تتكون من عدة خانات طويله هي بالنسبة لنا ليست بذات أهمية ولكننا لو أدركنا بأن تلك الأرقام ماهي في حقيقة الأمر الا إنعكاس للشريط الممغنط الظاهر بالجهة الخلفية لبطاقة الــ ATMوهذا الشريط هو حلقة الوصل بيننا وبين رصيدنا بالبنك الذي من خلاله تتم عملية السحب النقدي لأدركنا اهمية التخلص من المستند الصغير بطريقة مضمونه ونقصد بالضمان هنا عدم تركها لهاكر محترف يمكنه استخراج رقم الحساب البنكي بل والتعرف على الأرقام السرية للبطاقة البنكية . ATM

آثار الاختراق:

1-تغيير الصفحة الرئيسية لموقع الويب كما حدث لموقع فلسطيني مختص بالقدس حيث غير بعض الشباب الإسرائيلي الصور الخاصة بالقدس إلي صور تتعلق بالديانة اليهودية بعد عملية اختراق مخطط لها، و أيضاً كما حصل موقع قناة الجزيرة الفضائية مؤخراً إثر

عرضها لصور الأسرى الأمريكيين على شاشتها و موقعها فقامت جهة ما باختراق موقعها و تعطيلها لأكثر من يوم كامل و غيرت الصفحة الرئيسة له بصورة العلم الأمريكي.

2-السطو بقصد الكسب المادي كتحويل حسابات البنوك او الحصول على خدمات مادية او اي معلومات ذات مكاسب مادية كأرقام بطاقات الائتمان والأرقام السرية الخاصة ببطاقات الـ ATM

3-اقتناص كلمات السر التي يستخدمها الشخص للحصول على خدمات مختلفة كالدخول الي الانترنت حيث يلاحظ الضحية ان ساعاته تنتهي دون ان يستخدمها وكذلك انتحال شخصية في منتديات الحوار ، أو الاستيلاء على بريد شخص ما.

المخترقون والهاكرز

تعريف الهاكرز:

أطلقت هذه الكلمة أول ما أطلقت في الستينيات لتشير الي المبرمجين المهرة القادرين على التعامل مع الكمبيوتر ومشاكله بخبرة ودراية حيث أنهم كانوا يقدمون حلولا لمشاكل البرمجة بشكل تطوعي في الغالب .

بالطبع لم تكن الويندوز او مايعرف بالـ Graphical User Interfaceاو GUI قد ظهرت في ذلك الوقت ولكن البرمجة بلغة البيسيك واللوغو والفورتوران في ذلك الزمن كانت جديرة بالأهتمام . ومن هذا المبداء غدى العارفين بتلك اللغات ومقدمي العون للشركات والمؤسسات والبنوك يعرفون الهاكرز وتعني الملمين بالبرمجة ومقدمي خدماتهم للأخرين في زمن كان عددهم لايتجاوز بضع الوف على مستوى العالم أجمع. لذلك فإن هذا الوصف له مدلولات إيجابية و لا يجب خلطه خطأ مع الفئة الأخرى الذين يسطون عنوه على البرامج ويكسرون رموزها بسبب إمتلاكهم لمهارات فئة الهاكرز الشرفاء .

ونظرا لما سببته الفئة الأخيرة من مشاكل وخسائر لا حصر لها فقد أطلق عليهم إسما مرادفا للهاكرز و لكنه يتداول خطأ اليوم وهو الكراكرز (crackers) .

كان الهاكرز في تلك الحقبة من الزمن يعتبرون عباقرة في البرمجة فالهاكر هو المبرمج الذي يقوم بتصميم أسرع البرامج والخالي في ذات الوقت من المشاكل والعيوب التي تعيق البرنامج عن القيام بدورة المطلوب منه .ولأنهم كذلك فقد ظهر منهم إسمان نجحا في تصميم وإرساء قواعد أحد البرامج المستخدمة اليوم وهما دينيس ريتشي وكين تومسون اللذان نجحا في اواخر الستينيات في إخراج برنامج اليونيكس الشهير الي حيز الوجود. لذلك فمن الأفضل عدم إطلاق لقب الهاكر على الأفراد الذين

يدخلون عنوة الي الأنظمة بقصد التطفل او التخريب بل علينا إطلاق لقب الكراكرز عليهم وهي كلمة مأخوذة من الفعل Crack بالإنجليزية وتعني الكسر او التحطيم وهي الصفة التي يتميزون بها .

أنواع الهاكر :

و لهم عدة انواع و يصنفون على مستويين الأول من حيث المجال:

(Cracker) :

هاكر يستخدم برامج او تقنيات في محاولات لاختراق الأنظمة او الاجهزه للحصول على معلومات سرية او للتخريب كا ختراق مزودات شركة و حذف او إضافة معلومات . وكان هذا الاسم يطلق على من يحاول إزالة أو فك الحماية التي تضيفها شركات إنتاج البرمجيات على برامجها لمنع عمليات النسخ غير القانوني، أما الأن ،تم تصنيف هذا النوع من المخترقين في فئه خاصة سميت بالقراصنة (Pirates)

(Phreak) :

هاكر يحاول التسلل بر الشبكات الهاتفيه اعتماداً على أساليب تقنية غير قانونية أو التحك بهذه الشبكات و يستخدم هؤلاء أدوات خاصة مثل مولدات النغمات الهاتفية. ومع تحول شركات الهاتف إلى استخدام المقاسم أو البدالات الرقمية عوضا عن الكهروميكانيكية القديمة، تحول هؤلاء إلى استخدام الأساليب البرمجية ذاتها التي يستخدمها الـCrackers مؤلفو الفيروسات.

يقوم هذا النوع من الهاكر بتصميم الفيروسات محبة في التخريب و تدمير الاجهزه و يعتبر المحللون النفسيون أن من ينتمي إلى هذا النوع من المبرمجين مصاب بمرض عقلي أو نفسي ، يدفعه إلى هذه العمليات التخريبية التي لا يجني منها أي فائدة شخصية ، ويعتبر هذا النوع من أخطر الانواع.

(Cypherpunks) :

يحاول هذا النوع من الهاكر الحصول على أدوات و خوارزميات التشفير المعقدة و القوية و توزيعها بصورة مجانية حيث تسمح هذه الادوات بإجراء عمليات تشفير لا يمكن فكها إلا باستخدام أجهزه كمبيوتر فائقة.

(Cyberpunk) :

تطلق هذه التسمية على كل من يستخدم مزيجا من الطرق المسبقة للقيام بعمليات غير قانونية.

(Anarchists) :

وهذا النوع هو الذي يروج معلومات مخالفة للقانون او مشبوهة على أقل تقدير مثل طرق ترويج صناعة المخدرات أو المواد المتفجرة أو قرصنة القنوات الفضائية و غيرها.

و المستوى التقسيمي الثاني من حيث الخبرة :

1-المحترفون : هم إما أن يكونوا ممن يحملون درجات جامعية عليا تخصص كمبيوتر ومعلوماتية ويعملون محللي نظم ومبرمجين

ويكونوا على دراية ببرامج التشغيل ومعرفة عميقة بخباياها والثغرات الموجودة بها. تنتشر هذة الفئة غالبا بأمريكا وأوروبا ولكن إنتشارهم بدأ يظهر بالمنطقة العربية (لايعني هذا أن كل من يحمل شهادة عليا بالبرمجة هو بأي حال من الأحوال كراكر) ولكنه متى ما اقتحم الأنظمة عنوة مستخدما اسلحته البرمجية العلمية في ذلك فهو بطبيعة الحال احد المحترفين .

2-الهواة : إما أن يكون احدهم حاملا لدرجة علمية تساندە في الاطلاع على كتب بلغات أخرى غير لغته كالأدب الإنجليزي او لديه هواية قوية في تعلم البرمجة ونظم التشغيل فيظل مستخدما للبرامج والتطبيقات الجاهزة ولكنه يطورها حسبما تقتضيه حاجته ولربما يتمكن من كسر شفرتها البرمجية ليتم نسخها وتوزيعها بالمجان . هذا الصنف ظهر كثيرا في العامين الآخرين على مستوى المعمورة وساهم في انتشاره عاملين . الأول: انتشار البرامج المساعدة وكثرتها وسهولة التعامل معها . والأمر الثاني: ارتفاع أسعار برامج وتطبيقات الكمبيوتر الأصلية التي تنتجها الشركات مما حفز الهواة على إيجاد سبل أخرى لشراء البرامج الأصلية بأسعار تقل كثيرا عما وضع ثمنا لها من قبل الشركات المنتجة .

ينقسم الهواة كذلك إلي قسمين :

1- الخبير: وهو شخص يدخل للأجهزة دون الحاق الضرر بها ولكنه يميل الي السيطرة على الجهاز فتجده يحرك الماوس عن بعد او يفتح مشغل الأقراص بقصد السيطرة لا أكثر .

2- المبتدئ: هذا النوع أخطر الكراكرز جميعهم لأنه يحب أن يجرب برامج الهجوم دون أن يفقه تطبيقها فيستخدمها بعشوائية لذلك فهو يقوم أحيانا بدمار واسع دون أن يدري بما يفعله .

المخترقون بالدول العربية :

للأسف الشديد كثير من الناس بالدول العربية يرون بأن الكراكرز هم أبطال بالرغم أن العالم كله قد غير نظرته لهم. فمنذ دخول خدمة الأنترنت للدول العربية في العام 1996 تقريبا والناس يبحثون عن طرق قرصنه جديدة وقد ذكرت آخر الإحصائيات بأن هناك أكثر من 80% من المستخدمين العرب تحتوي اجهزتهم على ملفات باتش وهي ملفات تسهل عمل الكراكرز .

آلية الاختراق

يعتمد الاختراق على السيطرة عن بعد Remote وهي لا تتم الا بوجود عاملين مهمين الأول البرنامج المسيطر ويعرف بالعميل Clientوالثاني الخادم Server الذي يقوم بتسهيل عملية الاختراق ذاتها .

وبعبارة أخرى لابد من توفر برنامج على كل من جهازي المخترق والضحية ففي جهاز الضحية يوجد برنامج الخادم وفي جهاز المخترق يوجد برنامج العميل .

تختلف طرق اختراق الأجهزة والنظم باختلاف وسائل الاختراق ، ولكنها جميعا تعتمد على فكرة توفر اتصال عن بعد بين جهازي الضحية والذي يزرع به الخادم (server) الخاص بالمخترق ، وجهاز المخترق على الطرف الأخر حيث يوجد برنامج المستفيد او العميل Client و ذلك عن طريق ثلاثة أساليب :

1- ملفات أحصنة طروادة Trojan:

لتحقيق نظرية الاختراق لابد من توفر بريمج تجسسي يتم إرساله و زرعه من قبل المستفيد في جهاز الضحية ويعرف بالملف اللاصق ويسمى (الصامت) أحيانا و هو ملف باتش patch صغير الحجم مهمته الأساسية المبيت بجهاز الضحية (الخادم) وهو حلقة الوصل بينه وبين المخترق (المستفيد).

كيفية الإرسال والاستقبال :

تقوم الفكرة هنا على إرسال ملف باتش صغير هذا الملف يعرف باسم حصان طروادة لأنه يقوم بمقام الحصان الخشبي الشهير في الأسطورة المعروفة الذي ترك امام الحصن وحين ادخله إليه الناس خرج من داخلة الغزاة فتمكنوا من السيطرة و الاستيلاء على الحصن . ملفنا الصغير الفتاك هذا ربما يكون اكثر خبثا من الحصان الخشبي بالرواية لأنه حالما يدخل لجهاز الضحية يغير من هيئته فلو فرضنا بأن إسمه Bush.exe وحذرنا منه صديق فأننا سنجده يحمل اسما اخرا بعد يوم او يومين . لهذا السبب تكمن خطورة احصنه طراودة فهي من جانب تدخل للأجهزة في صمت وهدوء ، ويصعب اكتشافها من جانب اخر في حالة عدم وجود برنامج جيد مضاد للفيروسات .

لاتعتبر احصنة طروادة فيروسات وإن كانت برامج مضادات الفيروسات تعتبرها كذلك فهي بالمقام الأول ملفات تجسس ويمكن أن يسيطر من خلالها المستفيد سيطرة تامه على جهاز الضحية عن بعد وتكمن خطورتها في كونها لاتصدر اية علامات تدل على

وجودها بجهاز الخادم .

كيفية الإرسال :

تتم عملية إرسال بريمجات التجسس بعدة طرق من اشهرها البريد الالكتروني حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر فيجد به برنامج الباتش المرسل فيظنه برنامجا مفيدا فيفتحه او أنه يفتحه من عامل الفضول ليجده لايعمل بعد فتحة فيتجاهلة ظانا بأنه معطوب ويهمل الموضوع بينما في ذلك الوقت يكون المخترق قد وضع قدمه الأولى بداخل الجهاز (يقوم بعض الأشخاص بحذف الملف مباشرة عند إكتشافهم بأنه لايعمل ولكن يكون قد فات الأوان لأن ملف الباتش من هذا النوع يعمل فورا بعد فتحة وإن تم حذفه.

هناك طرق أخرى لزرع أحصنه طروادة غير البريد الالكتروني كانتقاله عبر المحادثة من خلال برنامج الـ ICQ وكذلك عن طريق إنزال بعض البرامج من احد المواقع الغير موثوق بها . كذلك يمكن إعادة تكوين حصان طروادة من خلال الماكرو الموجودة ببرامج معالجات النصوص .

كيفية الإستقبال :

عند زرع ملف الباتش في جهاز الضحية (الخادم) فأنه يقوم مباشرة بالاتجاه إلى ملف تسجيل النظام Registry لأنه يؤدي ثلاثة امور رئيسية في كل مرة يتم فيها تشغيل الجهاز :

(1) فتح بوابة او منفذ ليتم من خلالها الاتصال

(2) تحديث نفسه وجمع المعلومات المحدثة بجهاز الضحية إستعدادا لأرسالها للمخترق فيما بعد وتحديث بيانات المخترق (المستفيد) في الطرف الأخر . تكون المهمة الرئيسية لملف الباتش فور زرعة مباشرة فتح منفذ إتصال داخل الجهاز المصاب تمكن برامج المستفيد (برامج الإختراقات) من النفوذ. كما أنه يقوم بعملية التجسس بتسجيل كل مايحدث بجهاز الضحية او انه يقوم بعمل اشياء اخرى حسب مايطلبه منه المستفيد كتحريك الماوس او فتح باب محرك السي دي وكل ذلك يتم عن بعد .

بوابات الأتصال: Ports

يتم الاتصال بين الجهازين عبر بوابات ports او منافذ اتصال وقد يظن البعض بأنها منافذ مادية في امكانه رؤيتها كمنافذ الطابعة والفأرة ولكنها في واقع الأمر جزء من الذاكرة له عنوان معين يتعرف علية الجهاز بأنه منطقة إتصال يتم عبره ارسال واستقبال البيانات ويمكن استخدام عدد كبير من المنافذ للاتصال وعددها يزيد عن 65000 يميز كل منفذ عن الاخر رقمه فمثلا المنفذ رقم

1001 يمكن اجراء اتصال عن طريقة وفي نفس اللحظه يتم استخدام المنفذ رقم 2001 لإجراء اتصال اخر .

التواصل :

قلنا بأن المخترق قد تمكن من وضع قدمه الأولى بداخل جهاز الضحية بعد زرع ملف الباتش به ورغم خطورة وجود هذا الملف بجهاز الضحية فأنه يبقى في حالة خمول طالما لم يطلب منه المخترق التحرك فهو مجرد خادم ينفذ ما يصدر له من اوامر ولكن بدونه لا يتمكن المخترق من السيطرة على جهاز الضحية عن بعد .

وحتى يتم له ذلك، فإن على المخترق بناء حلقة وصل متينة بينه وبين الخادم عن طريق برامج خاصة تعرف ببرامج الإختراق . من جانب اخر تبقى احصنة طروادة عديمة الفائدة إن لم يتمكن المخترق من التعامل معها وهي تفقد ميزتها الخطرة حالما يتم اكتشافها والتخلص منها . وهناك عامل ممتاز يساهم في تحقيق هذة الميزة فبرامج مضادات الفيروسات الجيدة تكتشف ملفات الباتش الحاملة لأحصنة طروادة وتمنعها من الدخول للأجهزة لهذا يؤكد كل من له إلمام بالمعلوماتية أن تزود دائما الأجهزة الشخصية ببرامج مضادات الفيروسات وتحديثها بين الحين والأخر لأنها الخطوة الأولى للوقاية من الاختراقات ، كذلك علينا أن نتعود على عدم تمكين عامل الفضول من الولوج الي أنفسنا فل انفتح اية

مرفقات للبريد الألكتروني مجهول المصدر مهما كانت المغريات

2- عن طريق IP Address :

ذكرت بأن ملفات الباتش الحاملة لأحصنة طروادة هي حلقة الوصل بين المخترق والضحية ، ولكن في واقع الأمر فإن ملفات الباتش ليست إلا طريقة واحدة لتحقيق التواصل . عند إتصالك بالأنترنت تكون معرض لكشف الكثير من المعلومات عنك كعنوان جهازك وموقعه ومزود الخدمة الخاص بك وتسجيل كثير من تحركاتك على الشبكة .ولاتتعجب كثيرا حين تعلم بأن كثيرا من المواقع التي تزورها تفتح سجلا خاصا بك يتضمن عنوان الموقع الذي جئت منه IP Addressونوع الكمبيوتر والمتصفح الذي استخدمته بل وحتى نوع معالج جهازك وسرعته ومواصفات شاشاتك وتفاصيل كثيرة .

مبدئيا عنوانك الخاص بالانترنت Internet Protocol او IP يكشف الكثير عنك فكل جهاز متصل بالشبكة يكون له رقم معين خاص به يعرف بأسم الـ IP Address وكل عنوان لموقع على الانترنت يترجم الي IP Address الخاص بمزود الخدمة وبأختصار يكون الـ IP كرقم هوية خاص بكل من يعمل على الأنترنت. حينما يتمكن مخترق محترف من معرفة رقم الـ IP الخاص بالضحية فأنه من خلالة يتمكن من الولوج الي الجهاز والسيطرة عليه خلال الفترة التي يكون فيها الضحية متصلا بالشبكة فقط ، ولكن هذا الخيار لايخدم المخترق كثيرا لأن السيرفر الخاص بمزود الخدمة يقوم بتغيير رقم الـ IP الخاص بالمشترك تلقائيا

عند كل عملية دخول للشبكة . يمكنك أن تجرب ذلك بنفسك بالطريقة التالية :
أثناء إتصالك بالشبكة ومن قائمة إبداء إختر تشغيل واكتب الأمر التالي في المستطيل الظاهر winipcfg : سيظهر لك عنوان الـ IPاكتبه في ورقة صغيرة واقطع اتصالك . أعد الأتصال مرة اخرى بالشبكة وقم بالأجراء السابق ستجد أن
عنوان الـ IP الخاص بك قد تغير .

3- عن طريق الكوكي Cookies :

يمكن ايضا تحقيق التواصل للأختراق عن طريق الكوكي Cookie وهي عبارة عن ملف صغير تضعة بعض المواقع التي يزورها المستخدم على قرصة الصلب .
هذا الملف به اليات تمكن الموقع الذي يتبع له جمع وتخزين بعض البيانات عن الجهاز وعدد المرات التي زار المستخدم فيها الموقع كما وأنها تسرع عمليات نقل البيانات بين جهاز المستخدم والموقع فالهدف الأساسي منها هو تجاري ولكنه يساء إستخدامة من قبل بعض المبرمجين المتمرسين بلغة الجافا Java فهذة اللغة لديها قدرات عالية للتعمق اكثر لداخل الأجهزة والحصول على معلومات اكثر عن المستخدم. لايفضل منع الكوكيز كليا ولكن يمكن فلترتها من خلال المتصفح او ببعض البرامج كالـ . (Guard Dog)
وبعد فإن آلية الاختراق تتم مبدئيا بوضع بريمج الخادم بجهاز الضحية ويتم الأتصال به عبر المنفذ port الذي فتحة للمستفيد

(المخترق) في الطرف الأخر ولكن حلقة الوصل هذة تنقصها المعابر وهي البرامج المخصصة للأختراق وهذة الأخيرة .

محمد إسماعيل محمد
becasod@hotmail.com
becaso_d@yahoo.com